IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF APPEALS AND INTERFERENCES
(Attorney Docket № 14177US02)

In the Application of:

Ed H. Frank

Serial No. 10/658,310

Filed: September 9, 2003

For: METHOD AND SYSTEM FOR PROVIDING MULTIPLE ENCRYPTION IN A MULTI-BAND MULTI-PROTOCOL HYBRID WIRED/WIRELESS NETWORK

Examiner: Carlton Johnson

Group Art Unit: 2436

Confirmation No. 2145

Electronically Filed on January 4, 2011

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from an Office Action dated July 28, 2010 ("Final Office Action"), in which claims 1-42 were finally rejected. The Appellant respectfully requests that the Board of Patent and Appeals and Interferences ("Board") reverses the final rejection of claims 1-42 of the present application. The Appellant notes that this Appeal Brief is timely filed within the period for reply that ends on January 04, 2011, pursuant to a petition for a one-month extension.

REAL PARTY IN INTEREST
(37 C.F.R. § 41.37(c)(1)(i))

Broadcom Corporation, a corporation organized under the laws of the state of California, and having a place of business at 5300 California Avenue, Irvine, California 92617, has acquired the entire right, title and interest in and to the invention, the application, and any and all patents to be obtained therefor, as set forth in the Assignment recorded at Reel 014222, Frame 0368 in the PTO Assignment Search room.

RELATED APPEALS AND INTERFERENCES
(37 C.F.R. § 41.37(c)(1)(ii))

The Appellant is unaware of any related appeals or interferences.

STATUS OF THE CLAIMS
(37 C.F.R. § 41.37(c)(1)(iii))

The present application includes pending claims 1-42, all of which have been rejected. The Appellant identifies claims 1-42 as the claims that are being appealed. The text of the pending claims is provided in the Claims Appendix.

STATUS OF AMENDMENTS
(37 C.F.R. § 41.37(c)(1)(iv))

The Appellant has not amended any claims subsequent to the final rejection of claims 1-42 mailed on July 28, 2010.

SUMMARY OF CLAIMED SUBJECT MATTER
(37 C.F.R. § 41.37(c)(1)(v))

The Appellant has inserted Figs. 3, 4 and 6 of the present application below, to illustrate several aspects of the invention.

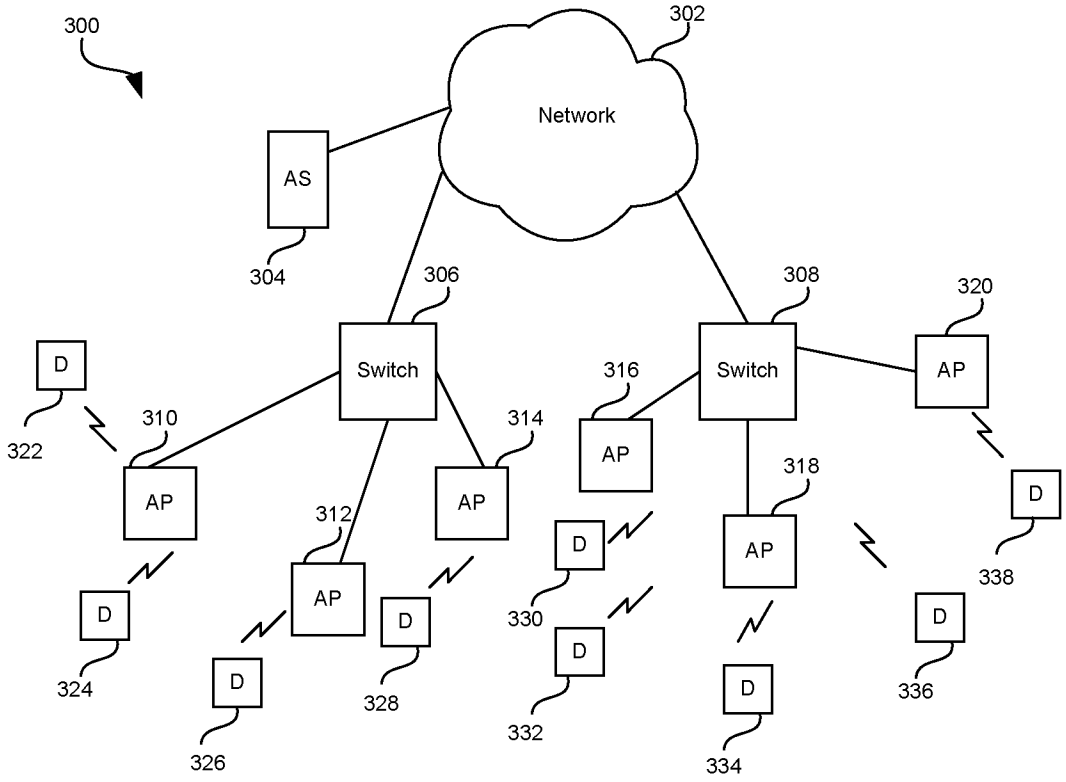

FIG. 3

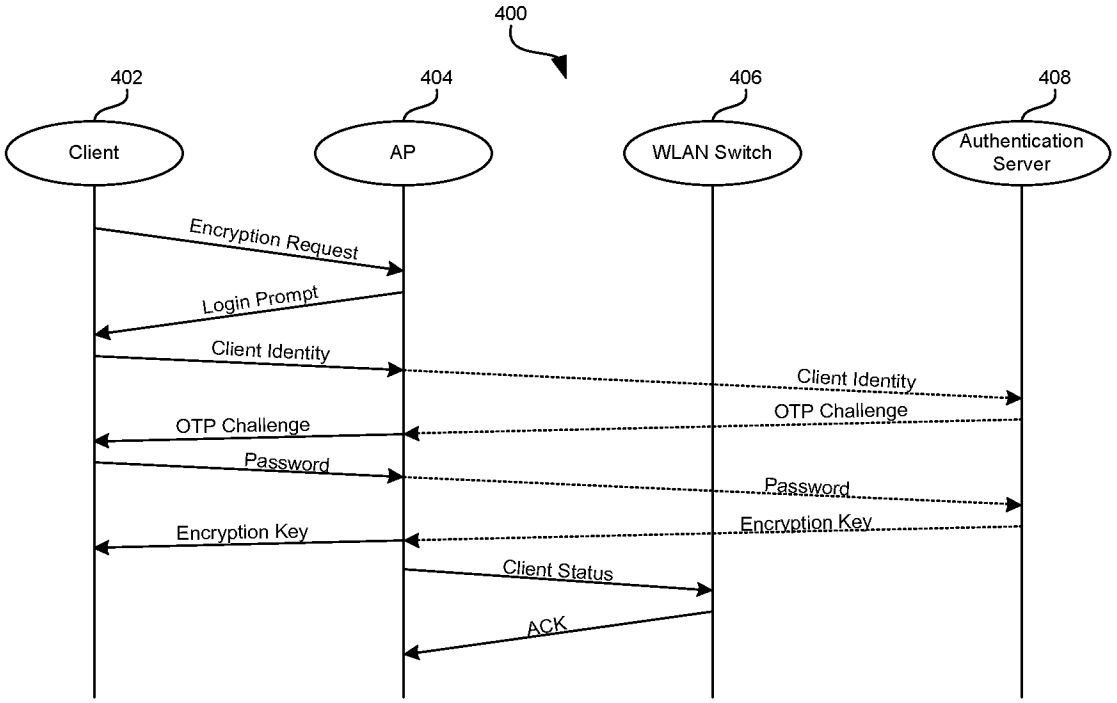
400
402
404
406
408
Client
AP
WLAN Switch
Authentication Server
Encryption Request
Login Prompt
Client Identity
Client Identity
OTP Challenge
OTP Challenge
Password
Password
Encryption Key
Encryption Key
Client Status
ACK

FIG. 4

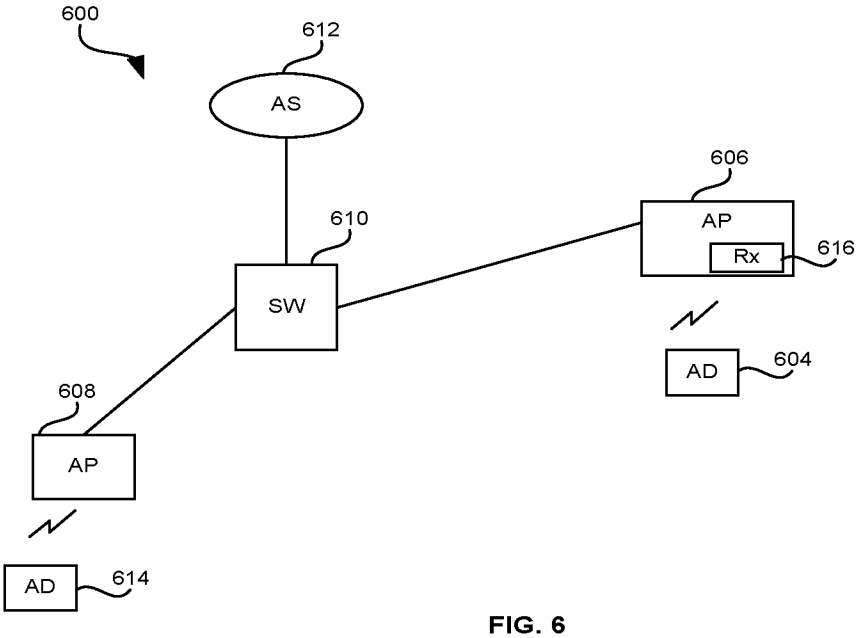
600
612
AS
606
610
AP
Rx
616
SW
AD
604
608
AP
AD
614

FIG. 6

Independent claim 1 recites the following:

A method[1] for multiple encryption[2] in a multi-band[3] multi-protocol[4] hybrid wired/wireless network[5], the method comprising:

receiving[6] on a first PHY channel of an access point[7], a request for initiation of a communication session from an originating access device[8];

authenticating[9] said communication session by authenticating said originating access device using a second PHY channel[10]; and

hosting[11] said communication session over a third PHY channel, said third PHY channel established[12] between said access point and said originating access device[13].

---

[1] *See* present specification, e.g., p. 8, ¶20, ll. 1-8, also *see* Figs. 1-6.
[2] *See id.*, e.g., p. 8, ¶21, ll. 1-8, i.e., encryption request and issuing encryption key using an authentication server 304 in Fig. 3 or authentication server 408 in Fig. 4.
[3] *See id.*, e.g., pp. 3-4, ¶08, ll. 1-14, such as 2.4-2.4835 GHz, 5.15-5.35 GHz and 5.725-5.825 GHz etc.
[4] *See id.*, e.g., pp. 3-4, ¶08, ll. 1-14, such as 802.11b, 802.11a, 802.11g etc.
[5] *See id.*, e.g., p. 8, ¶20, l. 2, wired/wireless WLAN network.
[6] *See id.*, e.g., p. 9, ¶24, ll. 5-7, via the receiver of AP 404 in Fig. 4, also see receiver 616 in AP 606 in Fig. 6.
[7] *See id.*, e.g., p. 8, ¶20, ll. 4-5, p. 9, ¶24, ll. 5-7, via the first PHY channel of receiver of AP 404, also see encryption request from client 402 to AP 404 in Fig. 4.
[8] *See id.*, e.g., p. 8, ¶20, ll. 4-5, access device 324 in Fig. 3, also *see* client 402 sending an encryption request to the receiver (first PHY channel) of AP 404 in Fig. 4.
[9] *See id.*, e.g., p. 8, ¶21, ll. 7-8, p. 9, ¶25, ll. 1-9, via the authentication server 408 in Fig. 4.
[10] *See id.*, e.g., p. 8, ¶21, ll. 2-8, p. 9, ¶25, ll. 5-9, i.e., the authentication server 408 delivers the encryption keys to the client 402 (originating access device) via the first PHY or the second PHY channel (i.e., via the receiver of AP 404) in Fig. 4.
[11] *See id.*, e.g., p. 8, ¶20, ll. 7-8, ¶20, ll. 7-8, i.e., the receiver 616 of AP 606 in Fig. 6 establishes one or more virtual channels (i.e., via the first, second or third PHY channels) to facilitate the hosting of the communication session between the originating access device (i.e., client 402) and a terminating access device, such as access device 614 in Fig. 6 (see p. 9, ¶24, ll. 8-10, ¶26, ll. 5-7, p. 28, ¶81, ll. 5-10).
[12] *See id.*, e.g., p. 8, ¶20, ll. 7-8, ¶20, ll. 7-8, i.e., the third PHY channel being one of the virtual channels established on the receiver 616 of AP 606 in Fig. 6 (*see* p. 9, ¶24, ll. 8-10, ¶26, ll. 5-7, p. 28, ¶81, ll. 5-10).

Claims 2-14 are dependant directly or indirectly upon independent claim 1.

Independent claim 15 recites the following:

A machine-readable storage, having stored thereon, a computer program having at least one code section[14] for providing multiple encryption[15] in a multi-band[16] multi-protocol[17] hybrid wired/wireless network[18], the at least one code section executable by a machine for causing the machine to perform the steps comprising:

receiving[19] on a first PHY channel of an access point[20], a request for initiation of a communication session from an originating access device[21];

authenticating[22] said communication session by authenticating said originating access device using a second PHY channel[23]; and

hosting[24] said communication session over a third PHY channel, said third PHY channel established[25] between said access point and said originating access device[26].

---

[13] *See id.*, e.g., the receiver 616 of AP 606 in Fig. 6 establishes one or more virtual channels (i.e., via the first, second or third PHY channels) to facilitate the hosting of the communication session between the originating access device (i.e., client 402) and a terminating access device, such as access device 614 in Fig. 6 (see p. 9, ¶24, ll. 8-10, ¶26, ll. 5-7, p. 28, ¶81, ll. 5-10).
[14] *See id.*, e.g., pp. 8-9, ¶23, ll. 1-4, also *see* Figs. 1-6.
[15] *See id.*, e.g., p. 8, ¶21, ll. 1-8, i.e., encryption request and issuing encryption key using an authentication server 304 in Fig. 3 or authentication server 408 in Fig. 4.
[16] *See id.*, e.g., pp. 3-4, ¶08, ll. 1-14, such as 2.4-2.4835 GHz, 5.15-5.35 GHz and 5.725-5.825 GHz etc.
[17] *See id.*, e.g., pp. 3-4, ¶08, ll. 1-14, such as 802.11b, 802.11a, 802.11g etc.
[18] *See id.*, e.g., p. 8, ¶20, l. 2, wired/wireless WLAN network.
[19] *See id.*, e.g., p. 9, ¶24, ll. 5-7, via the receiver of AP 404 in Fig. 4, also see receiver 616 in AP 606 in Fig. 6.
[20] *See id.*, e.g., p. 8, ¶20, ll. 4-5, p. 9, ¶24, ll. 5-7, via the first PHY channel of receiver of AP 404, also see encryption request from client 402 to AP 404 in Fig. 4.
[21] *See id.*, e.g., p. 8, ¶20, ll. 4-5, access device 324 in Fig. 3, also *see* client 402 sending an encryption request to the receiver (first PHY channel) of AP 404 in Fig. 4.
[22] *See id.*, e.g., p. 8, ¶21, ll. 7-8, p. 9, ¶25, ll. 1-9, via the authentication server 408 in Fig. 4.
[23] *See id.*, e.g., p. 8, ¶21, ll. 2-8, p. 9, ¶25, ll. 5-9, i.e., the authentication server 408 delivers the encryption keys to the client 402 (originating access device) via the first PHY or the second PHY channel (i.e., via the receiver of AP 404) in Fig. 4.

Claims 16-28 are dependant directly or indirectly upon independent claim 15.

Independent claim 29 recites the following:

A system[27] for multiple encryption[28] in a multi-band[29] multi-protocol[30] hybrid wired/wireless network[31], the system comprising:

at least one receiver of an access point adapted to receive[32] on a first PHY channel[33], a request for initiation of a communication session from an originating access device[34];

at least one authenticator[35] adapted to authenticate said communication session by authenticating said originating access device using a second PHY channel[36]; and

---

[24] *See id.*, e.g., p. 8, ¶20, ll. 7-8, ¶20, ll. 7-8, i.e., the receiver 616 of AP 606 in Fig. 6 establishes one or more virtual channels (i.e., via the first, second or third PHY channels) to facilitate the hosting of the communication session between the originating access device (i.e., client 402) and a terminating access device, such as access device 614 in Fig. 6 (see p. 9, ¶24, ll. 8-10, ¶26, ll. 5-7, p. 28, ¶81, ll. 5-10).

[25] *See id.*, e.g., p. 8, ¶20, ll. 7-8, ¶20, ll. 7-8, i.e., the third PHY channel being one of the virtual channels established on the receiver 616 of AP 606 in Fig. 6 (*see* p. 9, ¶24, ll. 8-10, ¶26, ll. 5-7, p. 28, ¶81, ll. 5-10).

[26] *See id.*, e.g., the receiver 616 of AP 606 in Fig. 6 establishes one or more virtual channels (i.e., via the first, second or third PHY channels) to facilitate the hosting of the communication session between the originating access device (i.e., client 402) and a terminating access device, such as access device 614 in Fig. 6 (see p. 9, ¶24, ll. 8-10, ¶26, ll. 5-7, p. 28, ¶81, ll. 5-10).

[27] *See id.*, e.g., p. 9, ¶24, ll. 1-10, also *see* Figs. 1-6.

[28] *See id.*, e.g., p. 8, ¶21, ll. 1-8, i.e., encryption request and issuing encryption key using an authentication server 304 in Fig. 3 or authentication server 408 in Fig. 4.

[29] *See id.*, e.g., pp. 3-4, ¶08, ll. 1-14, such as 2.4-2.4835 GHz, 5.15-5.35 GHz and 5.725-5.825 GHz etc.

[30] *See id.*, e.g., pp. 3-4, ¶08, ll. 1-14, such as 802.11b, 802.11a, 802.11g etc.

[31] *See id.*, e.g., p. 8, ¶20, l. 2, wired/wireless WLAN network.

[32] *See id.*, e.g., p. 9, ¶24, ll. 5-7, via the receiver of AP 404 in Fig. 4, also see receiver 616 in AP 606 in Fig. 6.

[33] *See id.*, e.g., p. 8, ¶20, ll. 4-5, p. 9, ¶24, ll. 5-7, via the first PHY channel of receiver of AP 404, also see encryption request from client 402 to AP 404 in Fig. 4.

[34] *See id.*, e.g., p. 8, ¶20, ll. 4-5, access device 324 in Fig. 3, also *see* client 402 sending an encryption request to the receiver (first PHY channel) of AP 404 in Fig. 4.

a third PHY channel being adapted to facilitate hosting[37] of said communication session, said third PHY channel established[38] between said access point and said originating access device[39].

Claims 30-42 are dependant directly or indirectly upon independent claim 29.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

Claims 1, 6-9, 15, 20-23, 29 and 34-37 are rejected under 35 U.S.C. § 102(e) as being anticipated by USP 7,039,027 ("Bridgelall"). Claims 2-5, 10-11, 16-19, 24-25, 30-33 and 38-39 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Bridgelall in view of USP 6,088,451 ("He"). Claims 12-14, 26-28 and 40-42 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Bridgelall in view of USP 7,325,058 ("Sheth"). Claims 1, 6-9, 15, 20-23, 29 and 34-37 are rejected under 35 U.S.C. § 102(e) as being anticipated by Bridgelall. Claims 2-5, 10-11, 16-19, 24-25, 30-

---

[35] *See id.*, e.g., p. 8, ¶21, ll. 7-8, p. 9, ¶25, ll. 1-9, via the authentication server 408 in Fig. 4.
[36] *See id.*, e.g., p. 8, ¶21, ll. 2-8, p. 9, ¶25, ll. 5-9, i.e., the authentication server 408 delivers the encryption keys to the client 402 (originating access device) via the first PHY or the second PHY channel (i.e., via the receiver of AP 404) in Fig. 4.
[37] *See id.*, e.g., p. 8, ¶20, ll. 7-8, ¶20, ll. 7-8, i.e., the receiver 616 of AP 606 in Fig. 6 establishes one or more virtual channels (i.e., via the first, second or third PHY channels) to facilitate the hosting of the communication session between the originating access device (i.e., client 402) and a terminating access device, such as access device 614 in Fig. 6 (see p. 9, ¶24, ll. 8-10, ¶26, ll. 5-7, p. 28, ¶81, ll. 5-10).
[38] *See id.*, e.g., p. 8, ¶20, ll. 7-8, ¶20, ll. 7-8, i.e., the third PHY channel being one of the virtual channels established on the receiver 616 of AP 606 in Fig. 6 (*see* p. 9, ¶24, ll. 8-10, ¶26, ll. 5-7, p. 28, ¶81, ll. 5-10).
[39] *See id.*, e.g., the receiver 616 of AP 606 in Fig. 6 establishes one or more virtual channels (i.e., via the first, second or third PHY channels) to facilitate the hosting of the communication session between the originating access device (i.e., client 402) and a terminating access device, such as access device 614 in Fig. 6 (see p. 9, ¶24, ll. 8-10, ¶26, ll. 5-7, p. 28, ¶81, ll. 5-10).

33 and 38-39 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Bridgelall in view of He. Claims 12-14, 26-28 and 40-42 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Bridgelall in view of Sheth. See the Final Office Action at pages 2-14. The Appellant identifies claims 1-42 as the claims that are being appealed. The text of the pending claims is provided in the Claims Appendix.

Without conceding that Bridgelall qualifies as a prior art under 35 U.S.C. § 102, the Appellant respectfully traverses these rejections at least for the reasons previously set forth during prosecution and at least based on the following remarks.

ARGUMENT
(37.F.R. § 41.37(c)(1)(vii))

I. Summary of Appellant's Arguments

The Appellant submits that Bridgelall does not disclose or suggest "**receiving on a first PHY channel of an access point**, a request for initiation of a communication session from an originating access device," or "**authenticating** said communication session by authenticating said originating access device **using a second PHY channel**," or "**hosting said communication session over a third PHY channel**, said third PHY channel **established between said access point and said originating access device**,"

The Appellant initially points out that Appellant's Figs. 4 and 6 clearly disclose that the access point (i.e., AP 404 in Fig. 4 or AP 606 in Fig. 6) is disposed between the originating access device (i.e., client 402 in Fig. 4 or device 604 in Fig. 6) and the authenticating server (i.e., authenticating server 408 in Fig. 4 or authenticating server 612 in Fig. 6) and the terminating access device (i.e., device 614 in Fig. 6).

In other words, the originating access device (i.e., 604), the authenticating server (i.e., 612) and the terminating access device (i.e., 614) cannot directly communicate to each other, without communicating via the AP (606).

Appellant's specification (*see* paragraphs [26] and [81]) also discloses at least one receiver of the access point (i.e., receiver 616 on AP 606 in Fig. 6), which

establishes a plurality of the virtual channels between the originating device (i.e., client 402 in Fig. 4 or device 604 in Fig. 6) and the terminating access device (i.e., device 614 in Fig. 6), and each of the virtual channel is established via one of the "first PHY channel", the "second PHY channel" and the "third PHY channel" (which are responsible for performing the recited steps in Appellant's claim 1).

In other words, Appellant's specification discloses that the "first PHY channel", the "second PHY channel" and the "third PHY channel" (as recited in Appellant's claim 1), are all channels of the AP (i.e., AP 606 in Fig. 6), which may be established by the AP receiver (i.e., receiver 616) as the respective virtual channels.

More specifically, the Examiner is referred to the following exemplary citations of Appellant's specification. For example, Appellant's paragraph [24] states the following (emphasis added):

> "...The system may include **an access point having at least one receiver** which may be adapted to receive a request for initiating a communication session from an originating access device. The initiation request may be received on a first PHY channel of the access point. **The receiver may be adapted to acknowledge the received request on the first PHY channel**. At least one authenticator may be adapted to **authenticate the originating access device using a second PHY channel**. **The first PHY channel, second PHY channel and/or a third PHY channel** may be adapted to **facilitate hosting of the communication session**.

Appellant's ¶[24] discloses that the AP receiver (i.e., receiver 616 of AP 604 in Fig. 6) uses a first PHY channel to receive a request from an originating access device

(i.e., client 402 in Fig. 4) to initiate a communication session, and a second PHY channel is used to authenticate the originating access device (i.e., client 402 in Fig. 4).

Furthermore, Appellant's ¶[24] discloses that **a communication session may be hosted using any of the three PHY channels**, **i.e., the first PHY channel, the second PHY channel or the third PHY channel**. In other words, Appellant's ¶[24] at least discloses a dynamic configuration to all three PHY channels, where any one of the first PHY channel, the second PHY channel or the third PHY channel, may be adapted to host a communication session.

The Examiner is further referred to Appellant's ¶[26] (also *see* ¶[81]), which provides an example to such configuration, which is carried out by the AP receiver. Specifically, Appellant's ¶[26] (also *see* ¶[81]) states the following (emphasis added):

> "…The authenticator may distribute the generated encryption/decryption key via the second PHY channel and/or the third PHY channel. **The receiver may be adapted to establish one or more virtual channels** between the originating access device and a terminating access device. The receiver may be adapted to tunnel information between the originating access device and the terminating access device. Additionally, **the receiver may be configured to establish at least a portion of the virtual channel over at least a portion of one of the first PHY channel, the second PHY channel and the third PHY channel**. In another aspect of the invention, the authenticator may be integrated with a switch or access point or it may be coupled separately to the hybrid wired/wireless network as a stand-alone component.'

Appellant's ¶[26] clearly discloses that the same AP receiver (i.e., AP receiver 616 in Fig. 6) may establish one or more virtual channels to tunnel information (i.e., hosting a communication) between the originating access device (i.e., device 604 in Fig.

6) and the terminating access device (i.e., device 614 in Fig. 6). Since both the originating access device (i.e., device 604 in Fig. 6) and the terminating access device (i.e., device 614 in Fig. 6) cannot directly tunnel information to each other except via the AP 604, the AP receiver (i.e., receiver 616 of AP 604 in Fig. 6), therefore, facilitates the information tunneling (i.e., hosting the communication) by establishing one or more virtual channels over anyone of the three PHY channels (i.e., the first PHY channel, the second PHY channel and the third PHY channel) in the AP receiver (i.e., AP receiver 616 in Fig. 6).

Accordingly, the Appellant submits that the respective "first PHY channel", "second PHY channel" and "third PHY channel" (as recited in Appellant's claim 1), are channels of the AP receiver (which are established as the plurality of virtual channels by the AP receiver (i.e., receiver 616 of AP 604 in Fig. 6)).

Bridgelall, on the contrary, discloses just the exact opposite of Appellant's claim 1. More specifically, Bridgelall's Fig. 4 discloses that the RACH channel 336 (the alleged "first PHY channel"), the SDCCH channel 338 (the alleged "second PHY channel") and the FACCH/TCH channel 342 (the alleged "third PHY channel") are cellular channels of the radio device 242 (the alleged "originating access device"), which communicate to the cellular antenna 226 (see Fig. 2). Bridgelall simply does not disclose or suggest that any of the alleged first, second or third PHY channel communicates to the AP 202 (the alleged "AP").

Based on the foregoing rationale, the Appellant submits that Bridgelall does not disclose or suggest "**receiving on a first PHY channel of an access point**, a request for initiation of a communication session from an originating access device," or "**authenticating** said communication session by authenticating said originating access device **using a second PHY channel**," or "**hosting said communication session over a third PHY channel**, said third PHY channel **established between said access point and said originating access device**," as recited by the Appellant in independent claim 1. Therefore, Bridgelall does not anticipate Appellant's claim 1.

Rejection Under 35 U.S.C. § 102

II. Bridgelall Does Not Anticipate Claims 1, 6-9, 15, 20-23, 29 and 34-37

The Appellant now turns to the rejection of claims 1, 6-9, 15, 20-23, 29 and 34-37 under 35 U.S.C. 102(e) as being anticipated by Bridgelall.

With regard to the anticipation rejections under 102, MPEP 2131 states that "[a] claim is anticipated only if **each and every element** as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." See Manual of Patent Examining Procedure (MPEP) at 2131 (internal citation omitted). Furthermore, "[t]he identical invention must be shown in as complete detail as is contained in the ... claim." See id. (internal citation omitted).

A. Rejection of Independent Claims 1, 15, and 29

With regard to the rejection of independent claim 1 under 102(e), the Appellant submits that Bridgelall does not disclose or suggest at least the limitation of "receiving on a first PHY channel of an access point, a request for initiation of a communication session from an originating access device," or "authenticating said communication session by authenticating said originating access device using a second PHY channel," or "hosting said communication session over a third PHY channel, said third PHY channel established between said access point and said originating access device," as recited by the Appellant in independent claim 1.

The Appellant refers the Examiner to Appellant's arguments in the above section I, that Appellant's "first PHY channel", "second PHY channel" and "third PHY channel", **all refer to the respective PHY channels on the access point**, and **not** on the originating access device.

The Final Office Action (*see* pages 5-6) states the following (emphasis added):

> "Bridgelall discloses …
> a) receiving on a first PHY channel of an access point, a request for initiation of a communication session from an originating access device; (see Bridgelall col 6, lines 7-9: enables user to conduct communications via the network via an access point; col. 7, lines 33-36: **mobile unit (wireless device) posts a request to network via channel** 336)
>
> b) authenticating said communication session by **authenticating said access using a second PHY channel**; (see Bridgelall col 6, lines 7-9: enables user to conduct communications via the network **via an access point**; col. 7, lines 39 - 66: connection management service request via

> dedicated channel 338 or 340; authentication center provides authentication request to mobile over dedicated channel; **mobile initiates authentication response over dedicated channel**; response executes a cellular authentication and voice encryption algorithm; algorithm produces a registration authentication result which is provide to service provider)
>
> c) hosting said communication session over a third PHY channel, **said third PHY channel established between said access point and said originating access device**. (see Bridgelall col 6, lines 7-9: enables user to conduct communications via the network via an access point; col. 8, lines 4-9: network assigns traffic channel for transmission of user data; assignment command from network and assignment complete message from mobile; **communication on new channel 342**)"

The Examiner relies for support on Bridgelall's Fig. 2, and equates Bridgelall's WWAN 200 (i.e., GSM cellular communication between the radio device 242 and the antenna 226), the WLAN 201 (i.e., between the radio device 242 and the AP 202) and the Bluetooth network (i.e., between the radio device 242 and the Bluetooth headset 244) to Appellant's multi-band multi-protocol hybrid wired/wireless network. The Examiner also equates Bridgelall's radio device 242 to Appellant's "originating access devices", and Bridgelall's access point 202 to Appellant's "access point".

The Examiner, however, equates Bridgelall's RACH channel 336 to Appellant's "first PHY channel of an access point", Bridgelall's SDCCH channel 338 to Appellant's "second PHY channel of an access point", and Bridgelall's FACCH/TCH channel 342 to Appellant's "third PHY channel of an access point".

The Appellant respectfully disagrees, and points out that the Examiner's arguments are deficient at least for the following reasons:

(1) The Examiner is referred to Appellant's above arguments in section I. In brief, **Appellant's respective "first PHY channel", "second PHY channel" and "third PHY channel", are channels of the AP receiver (which are established as the plurality of virtual channels by the AP receiver (i.e., receiver 616 of AP 604 in Fig. 6)).**

Bridgelall, on the contrary, discloses just the exact opposite of Appellant's claim 1. More specifically, Bridgelall's Fig. 4 discloses that the RACH channel 336 (the alleged "first PHY channel"), the SDCCH channel 338 (the alleged "second PHY channel") and the FACCH/TCH channel 342 (the alleged "third PHY channel") are cellular channels of the radio device 242 (the alleged "originating access device"), which communicate to the cellular antenna 226 (see Fig. 2). Bridgelall simply does not disclose or suggest any of the alleged first, second or third PHY channel communicates to the AP 202 (the alleged "AP").

The Examiner in the Final Office Action (*see* page 4, argument 3.4) further states the following:

> "Applicant argues all channels are attached to radio or mobile device. Each channel has two endpoints. The mobile unit is one endpoint and the access point (which facilitates communications to other nodes in the network) is the other endpoint. **There is no disclosure that the other endpoint has to be the access point since the access point is only mentioned in the first claim limitation for Claim 1**."

(2) The Appellant does not dispute that all channels have two endpoints which facilitate communications to other nodes. But the Appellant disputes the Examiner's

allegation that "*both Appellant's disclosure and claim 1 only specify that that the access point communicates in the first endpoint (i.e., the "first, PHY channel"), but not the other two endpoints (i.e., the "second and third PHY channels")*".

The Examiner is again referred to Appellant's arguments in the above section I (also *see* ¶[24], ¶[26] and ¶[81] of Appellant's specification etc.), that **Appellant's respective "first PHY channel", "second PHY channel" and "third PHY channel", are channels of the AP receiver.**

Therefore, the Appellant maintains that both Appellant's specification and claim 1 support Appellant's argument that all three PHY channels are of the access point. Bridgelall discloses the exact opposite, namely, the alleged "first, second and third PHY channels" being of the originating access device. In this regard, Bridgelall does not anticipate Appellant's claim 1, and Appellant's claim 1 is submitted to be allowable.

(3) Even assuming, arguendo, that Appellant's claim 1 does not recite that the "first, second and third PHY channels" are channels of the AP receiver (which the Appellant maintains that claim 1 does), the Examiner's argument is still deficient. For example, the Examiner alleges that Bridgelall (see col. 6, lines 7-9, and col. 7, lines 33-36) discloses "**receiving on a first PHY channel of an access point, a request** for initiating communication session **from an originating access device**," as recited in Appellant's claim 1.

The Appellant respectfully disagrees and refers the Examiner to the following citation of Bridgelall (*see* col 6, lines 7-12):

> "A portable dual mode Radio 242 enables a user to conduct communications via the network 200 with the WLAN 201 via the access point 202 or the WWAN 200 via any of the antennas 226, 228, 230 according to strength of signal measurements. The dual mode Radio device 242 may be also adapted to communicate with Blue Tooth users 244."

Bridgelall in the above citation merely discloses that the radio device 242 (the alleged "originating access device") may conduct a communication (i.e., the alleged "establishing a communication session") via anyone of the three possible paths, namely, the WLAN 201 via the AP 202, the WWAN 200 via the cellular antenna 226 or via the Bluetooth network.

Bridgelall's Figs. 3-4 (also *see* col. 7, lines 33-36), nevertheless, disclose that the radio device 242 (the alleged "originating access device") establishes a call request (the alleged "initiating a communication session") with the GSM cellular network via the cellular antenna 226 using cellular RACH channel 336 (the alleged "first PHY channel"). In this regard, Bridgelall's AP 202 does not receive the call request via the cellular RACH channel 336 (the alleged "first PHY channel") from the radio device 242 (the alleged "originating access device").

Therefore, by equating Bridgelall's RACH channel 336 to the alleged "first PHY channel", the Examiner, in effect, has conceded that Bridgelall does not disclose or suggest "**receiving on a first PHY channel of an access point**, a request for initiation

of a communication session **from an originating access device**," as recited in Appellant's claim 1.

(4) Likewise, Bridgelall's Fig. 4 discloses that the FACCH/TCH channel 342 (the alleged "third PHY channel") for connecting the call (the alleged "hosting said communication session"), is established between the radio device 242 (the alleged "originating access device") and the cellular antenna 226. In this regard, Bridgelall's FACCH/TCH channel 342 (the alleged "third PHY channel") is not established between the AP 202 (the alleged "AP") and the radio device 242 (the alleged "originating access device").

Accordingly, Bridgelall also does not disclose or suggest "hosting said communication session over a third PHY channel, **said third PHY channel established between said access point and said originating access device**," as recited in Appellants claim 1.

Based on the foregoing rationale, the Appellant maintains that Brideglall does not disclose or suggest "**receiving on a first PHY channel of an access point**, a request for initiation of a communication session **from an originating access device**," or "**authenticating** said communication session by authenticating **said originating access device using a second PHY channel**," or "hosting said communication session over a third PHY channel, **said third PHY channel established between said access point and said originating access device**," as recited by the Appellant in independent claim 1.

The Appellant respectfully requests that the rejection of claim 1 under 35 U.S.C. 102(e) be withdrawn. Likewise, independent claims 15 and 29 are submitted to be allowable for the same rationale of independent claim 1.

B. Rejection of Dependent Claims 6-9, 20-23 and 34-37

Based on at least the foregoing, the Appellant believes the rejection of independent claims 1, 15 and 29 under 35 U.S.C. § 102(e) as being anticipated by Bridgelall has been overcome and requests that the rejection be withdrawn. Additionally, claims 6-9, 12-14, 20-23, 26-28, 34-37 and 40-42 depend directly or indirectly from independent claims 1, 15 and 29, respectively, and are, consequently, also respectfully submitted to be allowable.

B(1). Dependent Claims 6, 20 and 34

The Examiner states the following in the Final Office Action (see pages 6-7):

> "With Regards to Claims 6, 20, 34, Bridgelall discloses the method, machine-readable storage having stored upon a computer program having at least one code section, system according to claims 1, 15, 29, comprising **receiving an identification of said originating access device by said access point**. (see Bridgelall col. 7, line 61 - col. 8, line 2: message indicates type of service, user number, and identification of the mobile (wireless device))"

The Examiner is referred to Appellant's above argument (1)-(4), that Bridgelall (Fig. 4 and col. 7, line 61 - col. 8, line 2) discloses that the ID of the alleged "originating access device" is received by the cellular antenna 226, which is not the AP 202 (the

alleged "AP"). Therefore, Bridgelall does not disclose "receiving an identification of said originating access device **by said access point**," as recited in Appellant's claim 6. Claim 6 is submitted to be allowable. Claims 20 and 34 are similar to claim 6, and are also submitted to be allowable.

B(2). Dependent Claims 7-9, 21-23 and 35-37

Claims 8-9, 21-23 and 35-37 are submitted to be allowable based on their dependencies on claims 6, 20 and 34, respectively.

Rejection Under 35 U.S.C. § 103(a)

In order for a *prima facie* case of obviousness to be established, the Manual of Patent Examining Procedure, Rev. 6, Sep. 2007 ("MPEP") states the following:

> The key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious. The Supreme Court in KSR International Co. v. Teleflex Inc., 82 USPQ2d 1385, 1396 (2007) noted that the analysis supporting a rejection under 35 U.S.C. 103 should be made explicit. The Federal Circuit has stated that "rejections on obviousness cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness."

See the MPEP at § 2142, citing In re Kahn, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006), and KSR International Co. v. Teleflex Inc., 82 USPQ2d at 1396 (quoting Federal Circuit statement with approval). Further, MPEP § 2143.01 states that "the mere fact that references can be combined or modified does not render the resultant combination obvious unless the results would have been predictable to

one of ordinary skill in the art" (citing KSR International Co. v. Teleflex Inc., 82 USPQ2d 1385, 1396 (2007)). Additionally, if a prima facie case of obviousness is not established, the Appellant is under no obligation to submit evidence of nonobviousness:

> The examiner bears the initial burden of factually supporting any prima facie conclusion of obviousness. If the examiner does not produce a prima facie case, the applicant is under no obligation to submit evidence of nonobviousness.

See MPEP at § 2142.

III. The Proposed Combination of Bridgelall and He Does Not Render Claims 2-5, 10, 11, 16-19, 24, 25, 30-33, 38 and 39 Unpatentable

The Appellant now turns to the rejection of claims 2-5, 10, 11, 16-19, 24, 25, 30-33, 38 and 39 as being unpatentable under 35 U.S.C. §103(a) over Bridgelall in view of He.

Based on at least the foregoing, the Appellant believes the rejection of independent claims 1, 15 and 29 under 35 U.S.C. § 102(e) as being anticipated by Bridgelall has been overcome. He does not overcome the deficiencies of Bridgelall. Since claims 2-5, 10, 11, 16-19, 24, 25, 30-33, 38 and 39 are dependant directly or indirectly from independent claims 1, 15, and 29, respectively, the Appellant respectfully submits that the rejection of the dependent claims consequently be withdrawn and the claims 2-5, 10, 11, 16-19, 24, 25, 30-33, 38 and 39 be allowed.

A(1). Rejection of Dependent Claims 4-5, 18-19 and 32-33

Claims 4-5, 18-19 and 32-33 are submitted to be allowable based on the same rationale as Appellant's arguments (1)-(2), namely, Bridgelall's authentication information is received via the alleged "second PHY channel", which is not of the AP 202.

A(2). Rejection of Dependent Claims 10, 24 and 38

The Examiner states the following in page 4 of the Final Office Action:

> "… He discloses wherein comprising generating at least one encryption/decryption key. (*see* He col. 18, lines 2-5; col. 19, lines 8-11; col. 20, lines 57-61: generation encryption/decryption key)"

The Examiner relies on He (*see* He col. 18, lines 2-5; col. 19, lines 8-11; col. 20, lines 57-61) to disclose the deficiency of Bridgelall, namely, "generating at least one encryption/decryption key dependent on the determined traffic type," as recited in Appellant's claim 10.

Specifically, He discloses generating a temporary secret key to secure communication **between the user and the network access server**. He, nevertheless, still does not disclose that the generated encryption/decryption key between the user and network access server is "dependent on the determined traffic type," as recited in Appellant's claim 10. Accordingly, the Appellant maintains that He does not overcome the deficiency of Bridgelall. Claim 10 is submitted to be allowable. Claims 24 and 38 are similar to claim 10 in many respects, and are also submitted to be allowable.

A(3). Dependent Claims 11, 25 and 39

Claims 11, 25 and 39 are submitted to be allowable based on their dependencies on claims 10, 24 and 38, respectively.

IV. The Proposed Combination of Bridgelall and Sheth Does Not Render Claims 12-14, 26-28 and 40-42 Unpatentable

The Appellant now turns to the rejection of claims 12-14, 26-28 and 40-42 as being unpatentable under 35 U.S.C. §103(a) over Bridgelall in view of Sheth.

Based on at least the foregoing, the Appellant believes the rejection of independent claims 1, 15 and 29 under 35 U.S.C. § 102(e) as being anticipated by Bridgelall has been overcome. Sheth does not overcome the above deficiencies of Bridgelall. Since claims 12-14, 26-28 and 40-42 are dependant directly or indirectly from independent claims 1, 15, and 29, respectively, the Appellant respectfully submits that the rejection of the dependent claims consequently be withdrawn and the claims 12-14, 26-28 and 40-42 be allowed.

In addition, the Appellant points out that even though Sheth discloses the alleged "virtual channel", Bridgellal, nevertheless, would still not communicate via Sheth's alleged "virtual channel". More specifically, the Examiner is referred to Appellant's above arguments (1) to (4), that Bridgellal utilizes a cellular network, which is a completely different network from Sheth's wired telephone line network. In other words,

Bridgellal's cellular network cannot benefit from Sheth's alleged "virtual channel", which is a wired network.

In this regard, the Appellant maintains that Bridgellal and Sheth do not establish a prima facie case of obviousness to reject Appellant's claims 12-14, 26-28 and 40-42 under 35 U.S.C. 103(a). Therefore, Appellant's claims 12-14, 26-28 and 40-42 are submitted to be allowable.

The Appellant also reserves the right to argue additional reasons beyond those set forth above to support the allowability of claims 1-42.

CONCLUSION

For at least the foregoing reasons, the Appellant submits that claims 1-30 are in condition for allowance. Reversal of the Examiner's rejection and issuance of a patent on the application are therefore requested.

The Commissioner is hereby authorized to charge $540 (to cover the Brief on Appeal Fee) and any additional fees or credit any overpayment to the deposit account of McAndrews, Held & Malloy, Ltd., Account No. 13-0017.

Respectfully submitted,

Date: January 4, 2011

/ Frankie W. Wong /

Frankie W. Wong
Registration No. 61,832
Patent Agent for Appellant

CLAIMS APPENDIX
(37 C.F.R. § 41.37(c)(1)(viii))

1. A method for multiple encryption in a multi-band multi-protocol hybrid wired/wireless network, the method comprising:

receiving on a first PHY channel of an access point, a request for initiation of a communication session from an originating access device;

authenticating said communication session by authenticating said originating access device using a second PHY channel; and

hosting said communication session over a third PHY channel, said third PHY channel established between said access point and said originating access device.

2. The method according to claim 1, comprising generating at least one encryption/decryption key for use during said communication session.

3. The method according to claim 2, wherein said authenticating comprises requesting authentication information from an authentication server.

4. The method according to claim 3, wherein said authenticating comprises delivering at least a portion of said authentication information received from said authentication server to said originating access device via said second PHY channel.

5. The method according to claim 4, comprising delivering said at least one encryption/decryption key to said originating access device via one of said first PHY channel or said second PHY channel.

6. The method according to claim 1, comprising receiving an identification of said originating access device by said access point.

7. The method according to claim 6, wherein said identity of said originating access device is one or more of a WEP key, a MAC address, and/or an IP address.

8. The method according to claim 1, comprising acknowledging said received request on said first PHY channel.

9. The method according to claim 1, comprising determining a type of traffic generated by said originating access device on said first PHY channel.

10. The method according to claim 9, comprising generating at least one encryption/decryption key dependent on said determined traffic type.

11. The method according to claim 10, comprising distributing said generated at least one encryption/decryption key via one or both of said second PHY channel and/or said third PHY channel.

12. The method according to claim 1, comprising establishing at least one virtual channel between said originating access device and a terminating access device.

13. The method according to claim 12, comprises tunneling information between said originating access device and said terminating access device.

14. The method according to claim 12, comprising establishing at least a portion of said at least one virtual channel over at least a portion of one of said first PHY channel, said second PHY channel or said third PHY channel.

15. A machine-readable storage, having stored thereon, a computer program having at least one code section for providing multiple encryption in a multi-band multi-protocol hybrid wired/wireless network, the at least one code section executable by a machine for causing the machine to perform the steps comprising:

receiving on a first PHY channel of an access point, a request for initiation of a communication session from an originating access device;

authenticating said communication session by authenticating said originating access device using a second PHY channel; and

hosting said communication session over a third PHY channel, said third PHY channel established between said access point and said originating access device.

16. The machine-readable storage according to claim 15, comprising code for generating at least one encryption/decryption key for use during said communication session.

17. The machine-readable storage according to claim 16, wherein authenticating code comprises code for requesting authentication information from an authentication server.

18. The machine-readable storage according to claim 17, comprising code for delivering at least a portion of said authentication information received from said authentication server to said originating access device via said second PHY channel.

19. The machine-readable storage according to claim 18, comprising code for delivering said at least one encryption/decryption key to said originating access device via one of said first PHY channel or said second PHY channel.

20. The machine-readable storage according to claim 15, comprising code for receiving an identification of said originating access device by said access point.

21. The machine-readable storage according to claim 20, wherein said identity of said originating access device is one or more of a WEP key, a MAC address, and/or an IP address.

22. The machine-readable storage according to claim 15, comprising code for acknowledging said received request on said first PHY channel.

23. The machine-readable storage according to claim 15, comprising code for determining a type of traffic generated by said originating access device on said first PHY channel.

24. The machine-readable storage according to claim 23, comprising code for generating at least one encryption/decryption key dependent on said determined traffic type.

25. The machine-readable storage according to claim 24, comprising code for distributing said generated at least one encryption/decryption key via one or both of said second PHY channel and/or said third PHY channel.

26. The machine-readable storage according to claim 15, comprising code for establishing at least one virtual channel between said originating access device and a terminating access device.

27. The machine-readable storage according to claim 26, comprises code for tunneling information between said originating access device and said terminating access device.

28. The machine-readable storage according to claim 26, comprising code for establishing at least a portion of said at least one virtual channel over at least a portion of one of said first PHY channel, said second PHY channel or said third PHY channel.

29. A system for multiple encryption in a multi-band multi-protocol hybrid wired/wireless network, the system comprising:

at least one receiver of an access point adapted to receive on a first PHY channel, a request for initiation of a communication session from an originating access device;

at least one authenticator adapted to authenticate said communication session by authenticating said originating access device using a second PHY channel; and

a third PHY channel being adapted to facilitate hosting of said communication session, said third PHY channel established between said access point and said originating access device.

30. The system according to claim 29, wherein said at least one authenticator is adapted to generate at least one encryption/decryption key for use during said communication session.

31. The system according to claim 30, wherein said at least one authenticator is adapted to receive requests for authentication information.

32. The system according to claim 31, wherein said authenticator is adapted to deliver at least a portion of said authentication information received from said authentication server to said originating access device via said second PHY channel.

33. The system according to claim 32, wherein said at least one authenticator is adapted to deliver said at least one encryption/decryption key to said originating access device via one of said first PHY channel or said second PHY channel.

34. The system according to claim 29, wherein said at least one receiver is adapted to receive an identification of said originating access device by said access point.

35. The system according to claim 34, wherein said identity of said originating access device is one or more of a WEP key, a MAC address, and/or an IP address.

36. The system according to claim 29, wherein said at least one receiver is adapted to acknowledge said received request on said first PHY channel.

37. The system according to claim 29, wherein said at least one authenticator is adapted to determine a type of traffic generated by said originating access device on said first PHY channel.

38. The system according to claim 37, wherein said at least one authenticator is adapted to generate at least one encryption/decryption key dependent on said determined traffic type.

39. The system according to claim 38, wherein said at least one authenticator is adapted to distribute said generated at least one encryption/decryption key via one or both of said second PHY channel and/or said third PHY channel.

40. The system according to claim 29, wherein said at least one receiver is adapted to establish at least one virtual channel between said originating access device and a terminating access device.

41. The system according to claim 40, wherein said at least one receiver is adapted to tunnel information between said originating access device and said terminating access device.

42. The system according to claim 40, wherein said at least one receiver is adapted to establish at least a portion of said at least one virtual channel over at least a portion of one of said first PHY channel, said second PHY channel or said third PHY channel.

EVIDENCE APPENDIX

(37 C.F.R. § 41.37(c)(1)(ix))

(1) US Pat. No. 7,039,027 ("Bridgelall"), entered into record by the Examiner in the July 28, 2010 Final Office Action.

(2) US Pat. No. 6,088,451 ("He"), entered into record by the Examiner in the July 28, 2010 Final Office Action.

(3) US Pat. No. 7,325,058 ("Sheth"), entered into record by the Examiner in the July 28, 2010 Final Office Action.

RELATED PROCEEDING APPENDIX

(37 C.F.R. § 41.37(c)(1)(x))

The Appellant is unaware of any related appeals or interferences.